Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?

Timothy Thomas

FOREIGN MILITARY STUDIES OFFICE

Open Source, Foreign Perspective, Underconsidered/Understudied Topics

The Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas, is an open source research organization of the U.S. Army. It was founded in 1986 as an innovative program that brought together military specialists and civilian academics to focus on military and security topics derived from unclassified, foreign media. Today FMSO maintains this research tradition of special insight and highly collaborative work by conducting unclassified research on foreign perspectives of defense and security issues that are understudied or unconsidered.

Author Background

Mr. Timothy L. Thomas (BS, Engineering Science, USMA; MA, International Relations, University of Southern California) is a senior analyst at the Foreign Military Studies Office at Fort Leavenworth, Kansas. Mr. Thomas conducts extensive research and publishing in the areas of peacekeeping, information war, psychological operations, low intensity conflict, and political-military affairs. Mr. Thomas was a US Army foreign area officer who specialized in Soviet/Russian studies. His military assignments included serving as the Director of Soviet Studies at the United States Army Russian Institute in Garmisch, Germany; as an inspector of Soviet tactical operations under the Organization for Security and Cooperation in Europe; and as a brigade S-2 and company commander in the 82nd Airborne Division. Mr. Thomas is an adjunct professor at the US Army's Eurasian Institute; an adjunct lecturer at the USAF Special Operations School; and a member of two Russian organizations, the Academy of International Information and the Academy of Natural Sciences.

Previous Publication: This paper was originally published in the Journal of Slavic Military Studies, March 2014. It is being posted on the Foreign Military Studies Office website with permission from the publisher.

Journal of Slavic Military Studies, 27:101–130, 2014
ISSN: 1351-8046 print/1556-3006 online
DOI: 10.1080/13518046.2014.874845

Routledge
Taylor & Francis Group

Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?

TIMOTHY THOMAS
Foreign Military Studies Office

This article discusses new developments in Russia's information and cyber warfare concepts. It updates information based on old paradigms and introduces several new developments that are influencing the current paradigm. It examines the potential shape of Russia's cyber strategy and offers a prediction as to how they might 'cyber cope' in future conflict.

INTRODUCTION

Since the mid-1990s, two areas have highlighted Russia's approach to information warfare (IW). The first area is a two-pronged approach, one that breaks the topic into information-technical and information-psychological subject areas. Other countries include more elements in their concept of IW,

The views expressed in this article are those of the author and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense or the U.S. government.

The Foreign Military Studies Office (FMSO) assesses regional military and security issues through open-source media and direct engagement with foreign military and security specialists to advise army leadership on issues of policy and planning critical to the U.S. Army and the wider military community.

Timothy Thomas is an analyst at the Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas. He retired from the U.S. Army as a Lieutenant Colonel in the summer of 1993. Mr. Thomas received a B.S. from West Point and an M.A. from the University of Southern California. He was a U.S. Army Foreign Area Officer who specialized in Soviet/Russian studies, serving as the Director of Soviet Studies at the United States Army Russian Institute (USARI) in Garmisch, Germany and as an inspector of Soviet tactical operations under CSCE. Mr. Thomas has done extensive research and publishing in the areas of peacekeeping, information war, psychological operations, low-intensity conflict and political military affairs. His three books are *Dragon Bytes, Cyber Silhouettes* and *Decoding the Virtual Dragon*.

Address correspondence to ATIN-F Timothy Thomas, FMSO, 731 McClellan Avenue, Ft. Leavenworth, KS 66027. E-mail: timothy.l.thomas20.civ@mail.mil

such as operational security, electronic warfare and other subjects. On the one hand, Russia has continued to do well in the information-technical arena. There is a multitude of young and resourceful code writers who have continued to keep the nation in the top echelon of those writing computer viruses for attack or defense purposes. The information-psychological area, on the other hand, still worries Russia's leadership, as witnessed by its aggressive response to the recent 'Russian winter' (Russia's equivalent to the 'Arab spring' concept) Internet uprising. During the Russian winter campaign, netizens contested the legality of Prime Minister Vladimir Putin's run for a third term as president of Russia. On election day, Russian police clamped down hard on those protesters in the streets who were anti-Putin, arresting many of them.

The second area that has highlighted Russia's IW and cyber theory approach has been an international push to define information and cyber terminology and to introduce the terms into an international legal framework utilizing the United Nations (UN) and numerous other organizations. Russia has been one country at the forefront of preparing UN resolutions on information security since the mid-1990s. The primary reason for this focus is undoubtedly to find a mechanism to filter certain information and ways of viewing the domestic and international situation. A group of internal Russian documents (Information Security Doctrine, National Military Strategy, etc.) have helped define Russia's concept of information space (a term used in Russia instead of information 'domain'). An overall goal of this international push appears to be to protect the information-psychological aspect of IW mentioned above.

It should be noted that the term *information* is being used in the description of Russia's Internet and military policies. Some Russian analysts have switched to the term *cyber*, but for the majority of the people writing on the topic, the focus remains on information. For that reason, the term *information warfare* is used throughout this article. That is still the way the Russians perceive information conflict in the coming years.

This article will discuss the development and overall impact of information technology (IT) issues on military and civilian policies. The conclusions will focus on two areas. First, it will discuss how these issues have affected the strategic and doctrinal dimension of Russia's information policy. Second, it will examine how well Russia might cope (as an attacker or defender) in an information phase of any future conflict in which it might become involved.

NEW DEVELOPMENTS

During the past two years, a significant shift in the importance of information and social media has resulted in a slight shift in the pillars of information warfare for some Russian specialists. Instead of information-technical and information-psychological affairs, for example, the focus for some is now on

scientific-technical and political-psychological issues. Further, the last two years have seen an increase in the use of the term *asymmetric warfare* and in the methods for its conduct. The strategies and capabilities of Russian IT specialists have also been further uncovered and discussed. These issues make it clear that Russia is continuing to focus on IT as a key force in the conduct of future war, whether in peacetime or wartime. Peacetime IT use is designed to uncover vulnerabilities in threat systems or to conduct espionage. Wartime IT use is designed to ensure secure command and control capabilities.

Andrey Kokoshin

Andrey Kokoshin, a former Deputy Minister of Defense and former Secretary of Russia's Security Council, has advocated the further development of IW and cyber topics. He has stated that cyber war is an integral component of information war, giving it a subordinate role.[1] In a May 2011 article in *Independent Military Review*, Kokoshin, currently the chairman for the Council for Scientific and Technical Policy under the Russian Federation's Defense Ministry, stated that information conflict has scientific-technical, political-psychological, operational and organizational aspects, among other issues.[2] This appears to be an expansion of the old information-technical and information-psychological approach. He noted the following:

> Cyber war, including EW, is a means of reducing the "opponent's" real combat effectiveness, a means of disorienting and disinforming him, of fragmenting his command and control system. The enemy's will to resist should be crushed as a result of that effect in the time intervals necessary for seizing and holding the initiative—strategic, operational, and tactical.[3]

Reducing an opponent's efficiency and increasing the use of deceptive measures through command and control fragmentation lie at the heart of Kokoshin's statement.

Kokoshin's thoughts indicate that there is a now a larger scientific and political role that cyber war is playing in today's environment. The science aspect appears to include more emphasis on the human–computer interface and the increasing role of network-centric operations. The political aspect was underscored during the March 2012 presidential election in Russia, when the Internet played a key role in organizing an opposition to Prime Minister Vladimir Putin's presidential run. It should be expected that the Internet will continuously be scrutinized for its positive scientific progress as well as its

---

1 *Interfax-AVN* Online, 26 January 2011.

2 Viktor Litovkin, interview with Andrey Afanasyevich Kokoshin, 'Realities: Andrey Kokoshin States "We Will Think about the Future"', *Independent Military Review Online*, 20 May 2011.

3 *Ibid*.

ability to undermine morale. Alternate ways of thinking and alternate views on applying Russian laws and regulations are also to be considered.

Kokoshin also advocated the development of a 'critical mass' of specialists devoted to studying cyber war and information countermeasures. This is due to the increasingly important role that cyber issues are playing in both national and international security issues. It is becoming more and more important for cyber specialists to attain a dominant position in information space. Information operations, he adds, use information, psychological and physical influences on government personnel, as well as on economic and military command management bodies. Kokoshin believes that Russia must develop a strategy for IW and cyber war based on both Russian and other foreign countries' opinions on the matter.[4] This process appears to be underway, as military journals are full of articles on the development of command and control issues that utilize both Russian and Western concepts.

Russian Cyber Strategies and Capabilities

Interestingly, one of the first Russian cyber strategies was proposed over a decade ago by one of the country's preeminent IW theorists, Sergey P. Rastorguev. The strategy was eerily familiar to those studying Chinese strategy, as it took on the same form and content. In a book commissioned by the Security Council of Russia titled *Information War*, Rastorguev wrote about the attempts of a fox to persuade a turtle to take off his shell. The fox indicated that turtles could fly without that weight. This sounded just great to the turtle, who was tired of lugging around his 'house' everywhere he went. The fox, obviously, was after a tasty meal. Eventually, the fox did persuade the turtle to take off his shell. He did so by showing videos to the turtle of turtles flying. The moral of the story and essence of strategy is that IW is the purposeful training or persuasion of an enemy to get him to do something seemingly for himself but in actuality doing something that benefits you. Several Chinese explanations of strategy follow the same storyline, although a cat and a mouse are used in one of their versions of the concept. Granted, this is but one IW specialist's view on strategy, but Rastorguev is an influential theorist. The overall theme of his book is how to write algorithms that could inject subliminal messages into the minds of people.

David A. Fulghum, writing in March 2012 in *Aviation Week*,[5] discussed the cyber capabilities of Russia and a few other foreign nations. He quoted a senior U.S. official who spoke at the Air Force Association's 2nd Annual Cyber Conference in Washington, DC, on these capabilities. The official

---

[4] *Interfax-AVN* Online, 26 January 2011.

[5] David A. Fulghum, 28 March 2012, in a posting listed at http://www.aviationweek.com/aw/community/persona/index.jsp?newspaperUserId=29473&plckUserId=29473.

reportedly had been involved in classified airborne electronic and cyber warfare since the Vietnam War. Fulghum wrote that

> U.S. analysts have based their judgment on the forensic analysis of APT [advanced persistent threat] such as skills at getting through firewalls. They contend that in the upper category, the order of sophistication is Russia, Israel, and then some of the Chinese. The number of penetrations by the Chinese overwhelms all the others, but the Russians put more focus on sophisticated exploitation schemes.[6]

Sophisticated exploitation schemes appear to imply the use of strategies.

'If you look at the educational background of the Russian [cyber-] mafia, most of them came out of the Russian Academy of Sciences', the specialist says. 'They've had a strong focus for a number of years'.[7] Fulghum stated that the reason that Russia is rated higher than Israel in its cyber expertise is the size of Moscow's resources and its well-educated population. In a 2010 article in *The Atlantic*, author James Fallows supported this contention. Fallows wrote that U.S. cyber specialist James Lewis considers Russia the top cyber threat to the U.S. and several European nations. Thus, Russia's cyber capabilities are well documented and established.

Asymmetric Operations and Information Security

S. G. Chekinov and S. A. Bogdanov, writing in the Russian journal *Military Thought*, stated that the means of information influence can now achieve strategic results. A strategic information (or cyber) confrontation could thus play an important role in disorganizing a military and state's command and control mechanism. Here the focus appears more psychological, since the authors add that such influence can create public opinion, organize antigovernment demonstrations and implement other measures that lower an opposing side's resolve to resist. Further, the authors state that for the military security of the Russian Federation, asymmetric measures must be undertaken that are of a 'systemic, comprehensive nature, combining political, diplomatic, informational, economic, military, and other efforts'.[8] The authors note that in 2006 then-President V. V. Putin stated that Russia's responses must be based on intellectual superiority, responses that are asymmetrical and less costly.

For Russia, such asymmetric responses include the following: measures that induce apprehension in the opposing side concerning intentions and retaliatory steps; demonstrations of readiness and capabilities along a

---

6 *Ibid.*

7 *Ibid.*

8 S. G. Chekinov and S. A. Bogdanov, 'Asymmetric Operations to Ensure Russia's Military Security', *Military Thought* 3, 2010, pp. 13–22.

strategic sector, with unacceptable consequences for the aggressor; and operations that deter potential adversaries through convincing them of the futility of an attack. The proliferation of indirect, noncontact forms of employing troops and modes of operation, along with the use of systems based on new physical principles, will have a strong impact on the course and outcome of a war. Important strategic facilities to damage include command and control centers, major industrial enterprises, important communications facilities and installations posing a potential environmental and health hazard (e.g., dams, hydroelectric power stations and water systems). Inflicting such damage in nonmilitary spheres is an asymmetric measure. Consideration must be given to the incommensurability of the sides' correlation of forces, the use of prohibited means of waging armed conflict, and the inability of an adversary to reliably defend positions. The implication is that cyber warfare and its protracted nature, if applied in indirect or nontraditional ways, along with the attainment of small victories, can sometimes lead to strategic capitulation.

The authors also added the following:

> The inability of the majority of the world's countries in the current circumstances to fight globalization's most powerful military machine (primarily the US) on equal terms has led in recent years to an increase in the number of terrorist acts, armed conflict, and local wars. Their coalescence into a single antagonistic system is giving rise to a phenomenon designated asymmetric operations by military-political theoreticians. . .these operations differ in term of their content, duration, and the forms and modes of employment of forces and assets. . . [9]

It is surprising that such learned people as Chekinov and Bogdanov would consider that the power of the U.S. and other military machines are responsible for the proliferation of terrorist acts, armed conflict and local wars. This cause-and-effect rationale is hard to follow, since the same situation during the Cold War did not produce the same results. No blame is placed on extremism or other causes of war, such as those behind the conflagration in the former Yugoslavia. It is hard to comprehend their logic.

Symmetric and Asymmetric Opposition to Network-Centric Warfare

Russian authors do discuss the topic of network-centric warfare (NCW) and often do so through the framework of the U.S.'s use of the term. One set of authors defined the central task of U.S. NCW as the conduct of effects-based operations. The Russians have discussed counters to the US network-centric principle. In one article, three retired officers offered symmetrical and asymmetrical counters. They stated that to counter NCW

[9] *Ibid.*

symmetrically, three conditions must be fulfilled: creating a super-reliable communication medium to ensure the effective functioning of computer networks; implementing a spatially dispersed grouping of intelligence and command and control resources; and creating a dispersed program medium providing real time processing of information streams. Asymmetric counters to NCW were offered as well, such as the use of electromagnetic bombs, destruction of an air adversary over his own territory, the use of unmanned aerial vehicles (UAVs) against cruise missiles, infrastructure strikes (such as against global navigation systems resources), heavy UAV strikes, magnetic information carriers to destroy software and the use of weapons of mass destruction at brigade level. The authors hope to capitalize on the increasing potential to disorganize an enemy command and control system. Finally, until it is possible to achieve parity in network-centric technologies, Russia must only use 'manual' command and control at the tactical level, according to these three officers.[10] The Russians do not discuss the Chinese concept of integrated network-electronic warfare (INEW) with the same intensity.

Hackers

In 2009, Kara Flook, a writer for the American Enterprise Institute, described the rationale behind the number of Russian hackers and the progress they have made. She noted that Russia has so many qualified hackers due to the country's legacy of emphasizing math and science educational opportunities. This has resulted in the development of highly qualified software writers and hackers. Russian hackers have long been active. They began countering Chechen websites in the mid-1990s, and in 1999 they were involved in cyber espionage activities against the Pentagon. In 2006 they were implicated in cyber attacks against Ukrainian websites; in 2007 they orchestrated a three-week attack on Estonia; and in 2008 Russian hackers conducted attacks on Georgian websites. They have practical knowledge and experience. Hacker magazines such as *Khaker* and the magazine's website, xakep.ru, are allowed despite strict government control over the media. In February 2008, Russia surpassed China as the largest generator of malware, with Russia accounting for 27.9 percent compared to China's 26.5 percent. According to Oleg Gordievsky, a Soviet KGB defector, cyber attacks have been a part of Russian strategy for a long time. Russian authorities have offered some hackers caught in the act of pilfering digits the option of working for the government instead of receiving a prison sentence.[11]

---

[10] P. A. Dul'nev, V. G. Kovalev and L. N. Il'in, 'Asymmetric Opposition in Network-Centric Warfare', *Military Thought* 10, 2011, pp. 3–8.

[11] Kara Flook, 'Russia and the Cyber Threat', 13 May 2009, at http://www.criticalthreats.org/russia/russia-and-cyber-threat.

Any discussion of Russian hackers would be incomplete if the criminal organization known as the Russian Business Network (RBN) is not mentioned. Four names who Flook mentions as prominent members of RBN are Alexandr Boykov, Sergei Smirnov, Alexei Vasiliev and Sergei Astakov. These and other RBN surrogates may have played a key role in many attacks and espionage capers.[12] Since cybercrime is targeted mainly against foreign enterprises, Russian law enforcement officials have not paid as much attention as they should. This is the result of incapacity as much as apathy, Flook writes. Instead, they focus on internal issues.

Attacks from Russia have not ceased in either Europe or the U.S. There are literally hundreds of examples after the 2008 attack on Georgia to the present time. For example, in 2011 it was reported that Russian hackers ranked second in global cybercrime, earning some $4.5 billion. Most recently, on 12 May 2012, hackers shut down a U.S. online video company streaming live video of Moscow's protests against the inauguration of President Putin. The company was being used by Russian activists. Brad Hunstable, the company uStream's chief executive, said this was the third 'highly coordinated attack from Russia in six months'.[13] German cybercrime units still consider Russia the number one actor against its banks and other key financial facilities in the country.

MINISTRY OF DEFENSE'S CONCEPTUAL VIEWS AND OTHER INFORMATION-RELATED PROPOSALS

Russia has been at the forefront of proposals intended to influence international information security thinking for over a decade. In 1995 the country offered definitions of information war and information weapons at the UN that were later rejected by the US. In 2000 the Russian Security Council proposed an Information Security Doctrine for Russia that was accepted and implemented by the Kremlin. The proposal of Russian Foreign Ministry representative Andrey Krutskikh at a November 2011 conference in London thus comes as no surprise. Krutskikh focused on the necessity that the world community ensure international information security (IIS). He underscored two points: first, that he would be using the term *information* instead of the term *cyber* and second, that he would talk about treating the Internet and information and communications technologies (ICT) either separately or together. He apparently decided that IIS cannot be resolved separately, and ICT should not be used as a form or means of involvement in politico-military conflicts. An international forum is needed to resolve such problems. While the uninterrupted and safe use of the Internet is required,

12 *Ibid*.

13 Jennifer Preston, 'Russian Hackers Attack Live Streaming Video Sites,' *The New York Times*, 10 May 2012, at http://thelede.blogs.nytimes.com/2012/05/10.

it is also important to remember that ensuring information security must not suppress freedom, and the exercise of freedom must not jeopardize national security and sovereignty. Finally, Krutskikh noted that Russia has tried to stimulate international discussion of information security issues through two mechanisms: the Rules of Conduct disseminated on 12 September 2011 at the 66th Session of the United Nations Security Council, and the 21–22 September 2011 Convention on International Security presented in Yekaterinburg, Russia.[14]

This section now discusses the information-related sections of the following proposals:

- 2011—*Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space*
- 2011—*Code of Conduct*
- 2011—*Convention on International Information Security*
- 2010—*Military Doctrine*
- 2010—*East-West Conference*
- 2009—*National Security Strategy*

Conceptual Views

In 2011 the Ministry of Defense proposed a document known as the *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space*. This document defined terms that included, as in 1995 at the UN, information warfare and information weapons, among others. *Conceptual Views* also offered principles (legality, priority, integration, interaction, cooperation and innovation) to guide the activities of the Russian Federation's Armed Forces (RFAF) in information space. Issues that the Russian document emphasized included the following:

- Legality: respect for national sovereignty and noninterference in the internal affairs of other states;
- Priority: collect relevant and reliable information regarding threats, protect information resources;
- Integration: utilize a coordinated and unified system to enhance the capabilities of the entire system;
- Interaction: coordinate defense activities with other federal executive bodies;
- Cooperation: develop cooperation on a global level to detect and prevent information and technological threats to peace, settle disputes involving these assets, build confidence in regard to the use of trans boundary information systems, and ensure the secure use of common information space;

[14] Remarks by Russian Foreign Ministry representative Andrey Krutskikh, Embassy of the Russian Federation in the United Kingdom of Great Britain and Northern Ireland (in English), 1 November 2011.

- Innovation: recruit skilled personnel; Russia's innovation centers must be able to develop and produce systems capable of carrying out activities in information space.[15]

The *Conceptual Views* further included rules for the use of information space when the latter is used as an agent of conflict deterrence, conflict prevention and conflict resolution:

- Deterrence and conflict prevention: develop an information security system for the RFAF that can deter and resolve military conflicts in information space; remain in a constant state of readiness; expand the group of partner states; conclude, under UN auspices, a treaty on international information security; establish control over the escalation of conflict; take priority steps to counter the development and spread of a conflict; neutralize factors leading to the conflict's spread; and shape public opinion means to limit the ability of instigators to further escalate the conflict.
- Conflict resolution: resolve information space conflicts primarily through negotiation and reconciliation; if in a crisis stage, exercise individual and collective self-defense rights not inconsistent with international law; deploy manpower and resources for ensuring information security on the territory of other states in the course of negotiations in accordance with international law; keep all media informed of the situation.[16]

The *Conceptual Views* included confidence-building measures that should be utilized, to include exchanging national concepts for ensuring information space security, as well as exchanging information promptly about crisis events. It was noted that Russia's defensive capability depends, to a large extent, on the effectiveness of Armed Forces activities in information space. Russia will do what it can to develop 'an international information security system in the interests of the entire global community'. This document follows the Russian government's 2000 Information Security Doctrine, the 2009 National Security Strategy, and the 2010 Military Doctrine, all of which touched on information issues. The latter two are discussed in the next section.

Code of Conduct

Russia, along with China, Tajikistan and Uzbekistan, was a signatory to the 12 September 2011 'Code of Conduct' letter addressed to the UN General Secretary, which offered an international code of conduct for information

[15] 'Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space', Ministry of Defense of the Russian Federation, 2011.
[16] *Ibid*.

security for the UNs' consideration. The code noted that efforts should be directed at providing developing countries with IT, that operations consistent with the objective of ensuring Internet stability is required and that policy authority for Internet-related public issues is the sovereign right of states. The latter issue is of particular concern to the U.S. State Department, since it implies that citizens of these countries will not have full access to the Internet, but only to those portions deemed essential by Russia and the other signatories. A few of the key portions and pledges of the text include:

- To not proliferate information weapons
- To respectfully comply with the diversity of social systems of all countries
- To endeavor to prevent other states from undermining the right of countries that have accepted the code of conduct
- To reaffirm the rights of states to protect their information space from disturbance
- To respect rights and freedom in information space on the premise of complying with relevant national laws and regulations
- To promote an Internet management system that facilitates access for all
- To lead all elements of society to understand their roles and responsibilities with regard to information security.[17]

The key questions regarding the code are 'which of these points take priority' and 'how are states to interpret statements like "protect information space from disturbance"?' What is considered to be a 'disturbance', that is, what is a free and open Internet a 'disturbance'? Will the rights and freedom of information space be respected, or will the requirement not to proliferate information weapons (which was not defined) take precedence and limit individual rights and freedoms? A detailed examination of what is considered information sovereignty and other such concepts is required before any Western nation would agree to the code of conduct as it is presently written.

Convention on International Information Security

The 2011 Convention on International Information Security at Yekaterinburg was presented to an international meeting of high-ranking officials responsible for security matters. Definitions were provided for various information-related terms.[18] Those for information warfare and information weapons are listed here, due to their contentiousness:

---

[17] 'Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General', Sixty-sixth Session of the United Nations General Assembly, 14 September 2011.

[18] The draft concept of the Convention on International Information Security can be found at isocbg-files.wordpress.com, listed as russ-draft-un-cyber-convention-english. All discussion on the Convention refers to this document.

> Information warfare—conflict between two or more States in information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures; undermining political, economic, and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents.
>
> Information weapon—information technology, means, and methods intended for use in information warfare.

Chapter 1, Article 1 of the Convention notes in subparagraphs that the Convention seeks to regulate the activities of governments to safeguard international information security and to ensure that the activity of governments in information space will be compatible with an individual's right to seek, receive and distribute information. However, the Convention further states, 'this right may be restricted through legislation to protect the national and social security of each State.' Respect must be maintained for the sovereignty of states and their existing political, historical and cultural specificities.

Eleven threats to peace and security in information space were listed.

- Use of IT to engage in hostile activity
- Purposefully destructive behavior in information space
- Illegal use of information resources of another government
- Actions that undermine the political, economic and social system of another government. Psychological campaigns carried out against the population of a state with the intent of destabilizing society
- Use of international information space for terrorist, extremist or other criminal purposes
- Dissemination of information across national borders in a manner counter to the principles and norms of international law
- Use of information infrastructure to disseminate information that inflames national, ethnic or religious conflict
- Manipulation of information flows in the information space of other governments to adversely affect the psychological or spiritual state of society
- Use of information means to the detriment of fundamental human rights and freedoms
- Denial of access to new information technologies
- Gaining of control over a state's national information resources.

The Convention then listed principles to follow to safeguard international information security. For example, each state has the right to develop its information space without external interference; aggressive information

warfare is deemed a crime against international peace and security; each State Party has the inalienable right to self-defense against aggressive actions toward it in information space; each state will make an attempt to achieve dominance in the information space over other states; and states can limit or interrupt access of its citizens to information space only when acting to protect national and social security.

There was an entire section of the Convention devoted to averting or resolving military conflicts in information space. This section included the following steps that states should take to avoid conflict in information space:

- Cooperate to ensure international information security
- Take steps to prevent any destructive information action originating from their territory
- Refrain from developing and adopting plans or doctrines capable of provoking information wars
- Refrain from actions aimed at a complete or partial breach of the integrity of information space
- Refrain from interfering within the internal affairs of another state
- Refrain from threatening to use force against another state's information space
- Refrain from encouraging the organization of any irregular forces to carry out activities in information space
- Refrain from slander or using hostile propaganda to interfere in the internal affairs of other states
- Take action against proliferating distorted messages that could interfere in another state's internal affairs
- Take action aimed at limiting the proliferation of information weapons.

Other chapters in the document were aimed at preventing terrorist use of information space, at counteracting illegal activities in information space and at cooperating in the sphere of international information security through confidence-building activities or consulting activities.

Treaty Recommendations

Russia has continually been at the forefront of attempting to define components of information and now cyber thought. At an East-West conference in 2010, Russian Dmitry I. Grigoriev, who works closely with the information security specialists at Lomonosov State University, stated that the first Russian step toward cyber security was the creation of a unifying terminology, which would enable all participants to speak the same language.

With regard to the contemporary situation, Grigoriev noted that threats to information and communication technologies now can achieve political

objectives. Special units in some nations conduct cyber warfare, and it is hard to avert anonymous attacks that can be cross-border in nature. Grigoriev called for the International Telecommunication Union to take over Internet governance, for the adoption of a universal international political-legal pact to coordinate the use of the Internet for military-political purposes, and for the creation of a regional information security system. Russia must also develop a mechanism to identify any hostile users of information technologies. He noted that Russia must comply with the principles of the sovereign equality of states and noninterference in their internal affairs. In summation, Grigoriev stated that the Russian Federation will sign legal pacts in the following areas: countermeasures against hostile use of information technologies; dissemination of cyber security standards; international cooperation in the conduct of research; and the creation of a mechanism for regular discussion at the expert level under the UN aegis for system problems to safeguard international information security.[19] Grigoriev's point of view was at the state or civilian level.

Military Doctrine

In 2010 Russia passed a new *military doctrine*.[20] This version of military doctrine was divided into sections that discussed military dangers and threats; the military policy of the Russian Federation; and military-economic support for defense. Information issues were not stated as an express external military danger, but rather as an internal military danger defined as the disruption of the functioning of organs of state power, of important state and military facilities, and of the information infrastructure of the Russian Federation. Any impediment to the functioning of state or military command and control systems was expressed as a main military threat. A 'characteristic' of contemporary military conflicts was noted to be the intensification of the role of information warfare. A 'feature' of modern military conflicts was stated to be the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force. High-technology devices to be used in future military conflicts include precision weaponry, electromagnetic weapons, lasers, infrasound weaponry, computer-controlled systems, drones and robotized models of arms and military equipment.[21]

According to the doctrine, Russia must possess the proper IT to deter conflict. A main task of the development of military organization was listed as improving the system of information support for the troops. With regard to military-economic support, the main task was to create conditions for

[19] Dmitry I. Grigoriev, 'The View from Russia: Russian Priorities and Steps Towards Cyber Security', East-West Institute Conference, April 2010.

[20] See http://www.carnegieendowment.org/publications/index.cfm?fa=view&id=40266.

[21] *Ibid*.

developing the military-technical potential at a level necessary for implementing military policy. This included developing forces and resources for information warfare, improving the quality of the means of information exchange using up-to-date technologies, creating new models of precision-guided weapons and developing information support for them.[22]

National Security Strategy

The strategy of May 2009 listed national security tools as the technologies and also the software, linguistic, legal and organizational items and telecommunication channels that transmit or receive information on the state of national security.[23] The concept was divided into the Contemporary World and Russia; Russia's National Interests and Strategic National Priorities; and Organizational, Normative-Legal, and Information Bases for Implementing the Present Strategy. Information issues that the document either discussed or highlighted included the following:

- The global information confrontation
- The use of information to enhance strategic deterrence
- The ability of information to present a threat to military security
- The illegal movement of narcotics and 'psychotropic substances'
- The preservation of information technologies and information focusing on the various issues of society's sociopolitical and spiritual life
- The development of information and telecommunications technologies such as computer hardware and electronics
- The proper use of the information-telecommunication medium
- The implementation of a series of information measures serving as the basis of this strategy: harmonizing the national information infrastructure with global information networks and systems; overcoming the technological lag in information science; developing and introducing information security technologies in the state and military administrative systems; increasing the level of protection of corporate and individual information systems; and creating a single information-telecommunications support system for the needs of the national security system.[24]

The document did not address in detail some of the salient concepts, such as how information would be used to enhance strategic deterrence; how information presents a threat to military security; and what is the proper use of information-telecommunication medium, among other issues.

---

22 *Ibid.*

23 Russian Federation Security Council Website, 12 May 2009.

24 A. A. Strel'tsov, *Gosudarstvennaya Informatsionnaya Politika: Osnovy Teorii* (Government Information Policy: Basic Theory), Moscow, MTsNMO, 2010.

Lomonosov Moscow State University Institute of Information Security Conferences

In 2012 the sixth information forum on information security (sponsored by Moscow State University) was held in Garmisch, Germany. The yearly event has two parts: the first is a conference in Garmisch, and the second is a conference in Moscow (or, as in 2011, in another country—in this case, China). The following are the topics discussed at these conferences in the past three years:

2010

- International cooperation, counteracting cyber terrorism; information warfare deterrence (only addition to this list since 2009), personal data protection, Internet governance mechanisms, and international cooperation in R&D

2011

- Concept of the international legal framework to regulate information (cyber-) space behavior; defining the source (organizer) of cyber attacks (scientific, technical, legal); international information security glossary; and content monitoring and filtering (to include preventing terrorist use of the Internet)

2012

- Classifying threats for UN documents; considering cyber espionage and intervention in internal affairs of another country as threats; relations between state responsibility for aggression and the authority for ruling in cyberspace; network sovereignty; types of international documents needed for information security; and the state of international relations regarding legal documents.

SOME ORGANIZATION AND SUBSTANCE-RELATED DEFENSE ISSUES

Russian theorists and analysts (some are listed below) have helped institute a series of reforms in the defense sector over the past several years that focus on the application of information concepts. First, it appears that MOD closely watched developments in other countries. Now, the ministry is considering the creation of a cyber command and the introduction of an organization similar to the Defense Advanced Research Projects Agency (DARPA). A lengthy discussion of the pros and cons of the network-centric concept has taken

place on the pages of journals such as *Military Thought*. An intense focus on the use of precision-guided weapons, UAVs and command and control issues has occurred, along with website and software upgrades. Finally, the Russian leadership is beginning to discuss the development of technologies that use IT but are actually beyond cyber—electromagnetic pulse, rail guns and other technologies.

Ministry of Defense Website Upgrade

In January 2012 the Defense Ministry announced it would be upgrading its website. The purpose is to shape a positive attitude toward the Armed Forces and Defense Ministry activities. IT experts hope for the following: over 10 million persons online simultaneously; from one to five million users viewing video relays simultaneously; 100,000 users able to work with a search engine and database; and several thousand people able to play 3D online games. Viktor Ryasnov, the IT specialist of the Department for the Development of Information Technology, stated that the new website assembles network resources currently contained on several sites. Further, the website will allow officers to view the construction progress being made on their own apartments.[25] This appears to be a way to strengthen the information-psychological stability of soldiers.

Command and Control Issues

President Dmitriy Medvedev, in a 20 March 2012 expanded meeting of the Defense Ministry Board of the Russian Federation, noted that it is imperative for RFAF to complete 'the creation of a new Armed Forces control system, especially at the brigade and tactical level'.[26] This system should be integrated into a single information space based on modern information and telecommunications technologies. Russia has been slowly developing command and control equipment over the past several years.

The issue of command and control is of vital importance to the RFAF. It plays a priority role in the development of Russian IW thought. Information superiority and information dominance, two key Western concepts, play subordinate roles. For example, Oleg Falichev, a journalist for the *Military-Industrial Courier* Online, interviewed Colonel General Arkadiy Bakhin, commander of the Western Military District, and Sergey Glazyev, academician at the Russian Academy of Sciences and Director of the Institute of the New Economy at the State Management University, on command and control issues. They noted that the creation of a system for the command

---

[25] Denis Telmanov and Artem Kuybida, 'Armed Forces: Defense Ministry Has Stormed the Internet', *Izvestiya* Online, 15 January 2012.

[26] Russian Presidential website, 20 March 2012 (in English), at http://www.kremlin.ru.

and control of mixed-branch force groupings in a strategic sector is a vital necessity. Furthermore,

> It is our profound conviction that victory in a future war will belong not to whoever has the most sophisticated tank or the fastest and most maneuverable fighter and most powerful missile, but to whoever is able, with the greatest effectiveness and coordination, to command and control the entire array of his own—albeit not even the most advanced—land, air, sea, and space-based information armaments.[27]

Russian Cyber Command

On 21 March, *RIA-Novosti* wrote that Russian authorities are discussing the creation of a cyber command in the armed forces. This command, according to the report, would safeguard information security in the armed forces and across the entire infrastructure of the state. Further, the *Novosti* report indicated that Russia is setting up an organization that is the equivalent of DARPA.[28] Colonel Sergey Ivanov, in an interview with *Ekho Moskvy* Online, stated that while it is difficult to say that a structure similar to DARPA already exists, it can be said that the Ministry of Defense has a military-scientific committee and a Directorate for Future Research. There is also a section for applied problems at the Russian Academy of Sciences. Most likely, Ivanov noted, these three structures have borrowed something from DARPA already.[29]

Principal Authors

The key voices in Russia's open-source thinking and advocating cooperation on information- and cyber-related topics are found at conferences and in journals. Among conference attendees, a key role belongs to Vladislav Sherstyuk, currently the Director of the Information Security Institute at Moscow State University. Sherstyuk has long had a voice in Russian communication and information issues. He was the Director of the Federal Agency for Government Communications and Information (FAPSI), the equivalent U.S. organization being the National Security Agency. In Soviet times, he helped establish the Lourdes listening post in Cuba in order to eavesdrop on U.S. communications. He helped coauthor the 2000 Information Security Doctrine of Russia while serving as First Deputy Secretary of the Security Council of Russia. Now he consults for the Kremlin on information security issues in a variety of fields in Russia and abroad.

---

[27] Oleg Falichev, 'From Assurances of Friendship to Concrete Actions', *Military–Industrial Courier* Online, 29 February 2012.

[28] *RIA-Novosti*, 21 March 2012.

[29] S. Buntman and A. Yermolin's interview with Sergey Ivanov, 'Military Advice', *Ekho Moskvy* Online, 10 March 2012.

A second key player who has been in the news often in 2012 is Major General Igor Sheremet, chairman of the Armed Forces Military Science Committee and Deputy Chief of the Russian Federation's General Staff. For the past 13 years, Sheremet was a professor at the N. E. Bauman Moscow State Technical University and chairman of the State Accreditation Commission at that university for the specialty 'information security'. The main areas of Sheremet's work in military science are research in the following areas: advanced forms and methods of armed struggle and the armed forces organizational development; advanced approaches to resources; and research into the nature of advanced means of armed struggle and creating these means for the defense industry complex. The committee uses hardware-software systems to support predictive computer modeling for armed confrontation at strategic, operational and tactical levels based on varying situations. Sheremet added that the institute has not been able to acquire a supercomputer with the performance of 'even one teraflop' in a 2012 article in *Moskovskiy Komsomolets*.[30] He added that military science must deal with cyber warfare and that several centers 'exist at the Defense Ministry and more broadly in our state's military organization' for work in this high-tech sphere.[31]

In another article, Sheremet discussed robotic warfare and NCW. With regard to robots, he stated that, in the future, he expects people to be used only where robots cannot be. He includes satellites and UAVs in this category. With regard to NCW, he mentioned the importance of the new army radio Azart, which provides access to any nearby network, realizing the network-centric concept in full, in Sheremet's opinion.[32] He is scheduled to discuss information technologies, nano-technologies and nontraditional weapons in the near future in an *Ekho Moskvy* interview.

Another information warfare specialist is Dr. Sergei Modestov. He has been researching, writing and teaching information warfare topics for a number of years. In an article in the *Journal of the Academy of Military Sciences,* Modestov stated that key information analysts, in his opinion, include Nikolai Ivanovich Turko, Boris Pavlovich Palchun, Nikolai Alekseyevich Kostin, Mikhail Alekseyevich Rodionov and Sergei Anatolyevich Komov.

Two other prominent authors are Vladimir Semenovich Pirumov and Sergey P. Rastorguev. Both have written extensively on information issues over the past 20 years. Pirumov, a retired admiral, was the scientific advisor to the Russian Security Council under President Boris Yeltsin and recently completed a book titled *Information Confrontation*. The book is written in Russian and English. Rastorguev has written several prominent works on

---

30 Viktor Malyutin, interview with Igor Sheremet, 'Planning and 3D Modeling. Weapon of New-Look Military Science', *Moskovskiy Komsomolets* Online, 30 March 2012.

31 *Ibid*.

32 Sergey Buntman and Anatoliy Yermolin, interview with Igor Sheremet, 'Voyennyy Sovet (Military Council) Program', *Ekho Moskvy* Online, 25 February 2012.

information topics. He is noted for his ability to precisely define terms in his work.

Many of the key authors of information- or cyber-related work write articles for the Russian Academy of Military Science's journal *Informatsionnye Voiny* (*Information Warfare*). The journal is published four times a year.

Related Departments Doing IW Work for Other Ministries

The old Department K unit of the Ministry of Internal Affairs (MVD) reportedly has been replaced by another department established on the basis of the existing department. The 16th Department of the Federal Security Service (FSB) is reportedly responsible for compiling a reserve force of hackers and using them to combat cybercrime or terrorism. Whether or not these hackers are conducting offensive or reconnaissance hacking or intrusions against the infrastructure of other nations is unknown.

Ministry of Defense Software

Reportedly the MOD has been using 'Dr. Web' to provide its antivirus software. According to *Wikipedia*, Dr. Web is a Russian antivirus company, as well as its flagship software suite. It was first released in 1992 and became the first antivirus service in Russia.[33]

The following article was posted on the Dr. Web website on 16 February 2012:

> Doctor Web—a Russian anti-virus developer company— is pleased to announce that it continues its cooperation with the Russian Ministry of Defense. A new agreement to supply anti-virus software under the state defense order in 2012 has been concluded. Dr. Web products have been successfully protecting Defense ministry PCs and file servers against viruses and other malicious software for over 15 years. The Russian Ministry of Defense has used the Dr. Web anti-virus since the mid 90s. It enabled the Ministry to create a centralized protection system shielding a significant number of its personal computers and servers against malicious software. The IT security software development license was first obtained by Doctor Web in 2005. In 2011 the Dr. Web Enterprise Security Suite was tailored for the Russian Defense Ministry project. Computers running the Mobile System of Armed Force were connected to the centralized anti-virus protection system. In 2012 within the cooperation framework servers will be incorporated into the defense system too.[34]

Igor Danilov is the Dr. Web CTO and founder.

---

[33] *Wikipedia* entry accessed on 14 May 2012 at http://en.wikipedia.org/wiki/Dr.Web.

[34] 'Dr. Web Protects Russian Defense Ministry', http://news.drweb.com/show/?i=2229&lng=en&c=14, 16 February 2012.

Communication Equipment in the Armed Forces

On 24 February 2012, the Russian paper *Independent Military Review* wrote that Russia finally had received an effective system of command and control at the tactical level. Author Gennadiy Starykh was referring to the Unified Tactical Echelon Command and Control System (ESU TZ). The task behind its creation was to develop an information-technical base for a tactical echelon command and control system that contained a modernization capacity, the possibility of scalability and adaptability for use, and an open architecture. This will allow one brigade with the ESU TZ to replace three similar ones with 20- or even 10-year-old equipment.[35]

Russia's communication system has been following a stage-by-stage development. The basic tasks included bringing the system into compliance with the structure of the command and control system and new configuration of the RFAF; maintaining the necessary level of combat and mobilization readiness; and creating and introducing standardized digital communications. Such equipment had to be compatible with the communications networks of the Russian Federation Unified Electronic Communications Network (RFYeSE). Meanwhile the RFAF's Main Communications Directorate began implementing the blueprint for creating a single information space to enable timely planning, coordination and feedback. Real-time planning and a single, integrated picture of the battlefield are crucial to success in the age of information. These developments include a system of new-generation satellite communications (YeSSS-3) with space complexes in geostationary and elliptical orbits.[36] Other systems being used are the joint troops command and control and weapons control system (YeSU TZ) and the Andromeda D (automated command and control system).

It was reported in 2010 that by late 2012, Russia's Army should be fully equipped with the Akatsiya-M mobile control and communications system, a military analog of the Internet. To date, three such systems, a RFAF General Staff's auxiliary control point and two other systems (HQ elements of the Voronezh Army and Moscow Military District) have been equipped with the Akatsiya-M. Every mobile point of the Akatsiya-M system is equipped with a UAV to support tactical-level operations in the forward edge. No updates since 2010 have been available in regard to this system.

In April 2012, new information on Russia's developing electronic warfare program was published. An article in *Independent Military Review* noted that the Borisoglebsk-2 complex is the basic armament for tactical formation electronic warfare (EW) units. The complex ensures the operation of all systems in signals intelligence and radio jamming modes via a

---

[35] Gennadiy Starykh, 'The TZ Exists: It Is Time to Take the Next Step', *Independent Military Review* Online, 24 February 2012.

[36] Vadim Bogachev, 'The Battlefield in the Palm of Your Hand. Single Information Space Being Created in Russia's Armed Forces', *Moskovskiy Komsomolets* Online, 29 February 2012.

single algorithm. The multifunction *Infauna* EW complexes are also being delivered to the armed forces. *Infauna* supports group protection against a radio-controlled explosive device and fire from close-combat weapons. A combat jamming transmitter, the *Lesochek*, supports the protection of armored personnel carriers. The impact of these systems has changed the objective of war to totally paralyzing a functioning adversary's command and control infrastructure, thereby rendering his decision making impossible in the information-intelligence and information-technology spheres.[37]

Beyond Cyber

Vladimir Fortov, director of the United Institute of High Temperatures at the Russian Academy of Sciences, stated that his institute is developing electromagnetic weapons, a nonlethal weapon in his opinion. The concept for this weapon is that 'a strong impulse of electromagnetic radiation hits a cruise missile or any other smart weapon and damages it. You can consider it an asymmetric answer or a strategic answer—as you wish'.[38] Acting Minister of Industry and Trade Denis Manturov stated that without state-of-the-art electronics, it is not possible to create model armaments. Russian Defense Minister Anatoliy Serdyukov said the Defense Ministry is creating weapons based on new physical principles.[39] It is a well-known fact that Russia is developing rail guns as well.

THE CONTINUATION OF INFORMATION-PSYCHOLOGICAL ISSUES

The impact of social media was most evident during the run-up to the election of Vladimir Putin as president of Russia in 2012. Never before has the number of critiques and demonstrations against the 'selected one' been so significant and public. Russian authorities will be faced with this dilemma in the coming years and will have to make hard choices as to their response mechanisms. Further, the Russian proclivity to discuss nonlethal and cognitive attacks on the psychological processes of citizens has not abated. In fact, the developments they discuss are more specific than in the past. The potential development of 'blocking childbearing functions of members of defined national or racial groups'[40] is but one example.

---

[37] Azret Bekkiyev, 'New Technologies in the Intense Light of Sozvezdiye', *Independent Military Review* Online, 6 April 2012.

[38] 'Prime Minister Vladimir Putin meets with experts in Sarov to discuss global threats to national security, strengthening Russia's defenses and enhancing the combat readiness of its armed forces', Website of the Prime Minister of the Russian Federation (in English), 24 February 2012.

[39] Vladimir Mokhov, 'Task for the Future', *Red Star* Online, 28 March 2012.

[40] Vasiliy Mikhaylovich Burenok, 'Armaments of the 21st Century will Have Intuition and Attitude. New Nano-Bio-Info-Cognitive Technologies Threaten Human Society', *Independent Military Review* Online, 2 December 2011.

Impact of the Loss of Ideology

As a result of the loss of communist ideology, a principal focus of the Russian leadership for over a decade has been on maintaining control of the flow of information in the country and measuring the impact of information flows on the conscience of the citizenry. Some still blame the fall of communism on what many Russians term the 'information-psychological' assault from the West, sometimes referred to as the so-called Third World War.

The collapse of the Soviet Union and the loss of all the trappings of communist ideology resulted in a tremendous loss of integrity and trust between the people and the governing elite. Russian leaders have worried about recapturing the minds and souls of its citizens ever since. A 2011 article in the Russian military newspaper *Red Star* is indicative of this trend and the requirement of the current leadership to develop a new *Weltanschauung* (worldview) for the people of Russia, especially its youth, which is resistant to negative factors.

The *Red Star* author offered the following advice, which, by his own admission, appears extremely radical:

> A system of boarding schools must be created, through which all children must pass. Let us say from the age of three. This system should be maximally closed off from the public by creating inspection membranes with unilateral conductivity. Children should know their country and their society, but there must be a mechanism for restricting their consciousness from foreign penetration.[41]

Nonlethal/Cognitive Attacks

Anatoliy Tsyganok, Director of the Center for Military Forecasting in Moscow, defines weapons with nonlethal effects as 'special technical means permitting effectively accomplishing political and peacekeeping missions; effectively participating in local conflicts; and achieving one's goals without inflicting excessive losses on the opposing side, with minimal victims among the civilian population and without significant destruction of material values or doing harm to the environment'. [42] He believes the U.S. defines the term as weapons 'created and employed chiefly for disabling personnel or materials while minimizing fatalities and prolonged injuries to personnel, as well as undesirable harm to those around them'.[43] He adds that in 20 years destructive, penetrating and fragmentation weapons will not be employed. In their place will be weapons that stop, calm or frighten people. He writes that the

---

41 El Murid (pseudonym), 'Information Wars', *Red Star*, 3–9 August 2011.

42 Roman Kretsul, Interview with Anatoliy Tsyganok, 'The Warfighting System is Changing: An Expert Evaluated Serdyukov's Statement on Developing Weapons of the Future', *Vzglya*d Online, 22 March 2012.

43 *Ibid*.

U.S. used stink weapons against the Taliban a few years ago and that the U.S. used a psychogenic weapon in Africa, employing a laser to write a message on a cloud or wall from God.[44] No sources are cited for these assertions.

Tsyganok added that future weapons would include infrasonic weapons below 16 hertz that disperse demonstrators by raising body temperatures. A geographic weapon is also under discussion. In the 1950s, there was an effort to shift tectonic plates via explosions, a weapon that today is known as a geomagnetic radiation weapon.[45]

It appears that Tsyganok's comments were in sync with an *Interfax* release that stated a 'program of development for weapons based on new physical principles after 2020 would be drafted by the end of 2012'. The program will cover beam, wave, genetic and psychophysical weapons, among others.[46] In 2011 retired Major General Vasiliy Mikhaylovich Burenok offered an even further extreme view of future weaponry. He discussed how 21st-century armaments will include several of Tsyganok's weapons and will have a human–technical interface as well. He stated:

> To investigate and understand human cognitive functions, and to model them on a computer is one of the most important tasks for modern science. The goal of this task is to provide the possibility of transferring the cognitive functions from the "biological elemental base" (the neural networks of the brain) to an electronic elemental base which can operate millions of times faster, has practically unlimited memory, etc.; and also to construct information (computation) equipment of the next level (generation).[47]

In particular, Burenok noted that with a lack of legal regulation of online networks, there will be a greater chance for psychological activities and the use of modern information-communication technologies to affect the consciousness of citizens. These activities can be used for information, political, economic or cultural expansion. Individual or mass neuroprogramming is also possible, Burenok noted, along with 'cellular design of known and new infections, damaging and ruining vitally important organs and sections of the human body', as well as 'blocking childbearing function of members of defined national or racial groups'.[48] Societies must conduct their own 'preparatory courses' for mastering these new areas of knowledge and for creating a system to respond to such threats.[49] The range of these activities under consideration is startling.

---

44 *Ibid*.

45 *Ibid*.

46 *Interfax* (in English), 22 March 2012.

47 Burenok, 'Armaments of the 21st Century will Have Intuition and Attitude. New Nano-Bio-Info-Cognitive Technologies Threaten Human Society'.

48 *Ibid*.

49 *Ibid*.

According to Burenok, armed violence will assume a secondary position in the future as different 'forms and methods of adversely influencing a state, a society, or an individual' will appear. Such developments include changing the 'technogenic shell' of civilization, making a distinction between living and nonliving things uncertain. Here the real issue is about cyber life, he notes. New gene combinations will be designed that do not currently exist, while nanobots will alter the characteristics of an organism. New conflicts will, in Burenok's opinion, not be so much 'wars between people as wars of artificial intellects and the equipment and virtual reality created by this kind of intellect'.[50]

Social Media

Worry over so-called information-psychological attacks has caused Russia to look at what is often termed 'soft power' issues associated with social media more closely than other countries. Government attempts to control digital media outlets have often backfired and resulted in displays of indignation from the population, such as the protests of early 2012 against then Prime Minister Vladimir Putin's run for the presidency. The Internet (known as *Runet* in Russia) has become the population's alternate source of news to state-controlled media. Some of the most popular social media outlets are *Vkontakte* and *Odnoklassniki*. The *Yandex* search engine and *LiveJournal* are two other popular sites.

Due to the growing influence of social media, the Kremlin worries about people like Rustem Agadamov, a popular blogger, and Alexei Navalny, the anticorruption blogger who orchestrated many of the demonstrations against Prime Minister Vladimir Putin's presidential aspirations. Navalny is the only opposition leader barred from state-controlled TV, and he has been characterized as a CIA operative, as Russia's leadership tends to brand people who oppose them. For Navalny, the Web offered a way to publicize his work on a *LiveJournal* blog. The Kremlin will be watching his every move in the coming months as he continues to discuss corruption at the highest level in Russia. He was arrested and released during the inauguration of Putin as the new president on 6 May.

Another focal point is the work of Alexander Kovalyev in the Ural Mountains, who edits his city's chief political opposition website from his apartment. Kovalyev used to work for the newspaper of Magnitogorsk's Iron and Metal Works. When he became fed up with the direction of the plant, he began writing for Pavel Verstov, who was in charge of a website that detailed some of the problems in the plant. The plant's spokesman, Vladimir Dryomov, stated that in Magnitogorsk the value of the reliability of a man like Putin is important and that the majority of the people support him.

---

50 *Ibid.*

And the Iron and Metal plant's response to the anti-Putin rallies around the country? A plant website noted that 'protests around the country were being triggered by a top-secret US military base in Alaska beaming high-frequency signals into the brains of Russians.'[51] Again, if one is not pro-Putin, then one must be a U.S. intelligence operative or under their influence. This tendency was further reinforced when Russia's state-controlled NTV produced a film indicating the U.S. State Department had coordinated the anti-Putin protests. The film caused outrage among Russian citizens who participated in the event.

Of course, there are also pro-government sites online that generate a nuanced rendering of the news. Supported by older generations and youth organizations (such as Nashi), the government has developed its own brand names on the Web. For news, *RIA Novosti* is popular, along with outlets such as *LifeNews.Ru*, which oligarchs such as Yuri Kovalchuk support to discredit opposition figures.

The government's Ministry of Communications reportedly is authorized to revoke any Internet service provider's license if one of the ministry's subordinate elements, Roskomnadzor, considers a site extremist. The Federal Security Service's System for Operative Investigative Measures (SORM-2) program can also monitor Internet and telephone connections without court approval, while Russia's largest domain registration center, *Ru-Center*, is informally controlled by the government. To further ensure control, President Putin has asked state companies to give priority to domestic vendors when purchasing IT. Putin has at his service an elaborate program of provocation, sanctions, hacking, videotaping and wiretapping to persuade people as well.

Journalists Andrei Soldatov and Irina Borogan discussed the Kremlin's information strategy in a March 2012 article. They wrote that in the late 2000s the Kremlin decided to resort to simple and crude methods, described as an aggressive invasion of liberal discussion forums, where vulgar and indecent language and insults were used to make people reluctant to use the sites. They also used 'Internet trolls' to insert unprintable language to scare away people criticizing the government. The accounts of opposition figures have been subjected to phishing attacks by hackers, who work anonymously. Most interesting was the discovery in February 2012 by Anonymous that money was being paid to pro-Kremlin bloggers and that distributed denial of service (DDoS) attacks were most likely organized by similar groups against opposition media. Rosmolodyozh, the Federal Youth Agency, appears to have an army of cyber activists who work in the blogosphere and social networks to carry out work for them. There is also Konstantin Rykov, an online pro-Kremlin activist, who has spent more than

[51] Alan Cullison, 'In Russian Steel Town, Putin Woos Voters with Jobs and an Iron Fist', *The Wall Street Journal*, 3–4 March 2012, pp. A1, A9.

a decade online working for the Kremlin using a variety of products, such as insults, bots, spam, jamming and so on.

Overall, the Kremlin's strategy appears to have had spotty success. In a *LiveJournal* rating for 12 March, no pro-Kremlin bloggers were in the top 20. Of course, a pro-Kremlin website rating may have just the opposite result. Political analyst Gleb Pavlosky, a former Kremlin spin doctor, feels that the Kremlin's strategy is effective so long as a power structure protects it. When the structure disappears, people begin whining. Such a strategy works in China but not in a competitive environment, according to Soldatov and Borogan.

IW/CYBER TERMINOLOGY AND INTERNATIONAL DEVELOPMENTS

A key focus of Russia's information approach for the past 15 years has been to demand a better information-related terminology guide. This includes defining terms such as *information warfare* and *information weapons* in particular. Russian efforts in this regard have spanned a host of countries and treaties, potential and realized. At a 2011 conference there was, for the first time, some agreement on a cyber-related lexicon of terms. A few months later, when the military's concept of information space was published, the lexicon used was once again focused only on information-related terms. Thus, as we enter 2012 it is still a wide open playing field in Russia as to where the terminology discussion will end up, with cyber or information playing the lead role.

On Terminology

With regard to the essence of cyber terminology from a military point of view, one Russian author defined cyberspace as an objective reality, a medium for computer functions in which one can affect an enemy's systems and protect one's own. In cyberspace, 'it turned out to be very convenient to "wash away" the boundaries between war and peace. In fact, one can inflict damage on an adversary without formally stepping across the boundary separating war from peace'.[52] A cyber attack was defined as a form of hostile action in cyber space aimed at cyber systems, information resources or an information infrastructure to achieve some goal, implemented with special programs, equipment and methods. Cyber war was defined as the systematic struggle in the cyber domain among states, political groups and extremist and terrorist groups, where targets are information resources and whose properties (integrity, accessibility and confidentiality) can be violated.[53]

---

52 P. I. Antonovich, 'On the Essence and Content of Cyber-War', *Military Thought* 7, 2011, pp. 39–46.

53 *Ibid.*

Russia–US Bilateral on Critical Terminology

There are several cyber terms that were defined at a 2011 U.S.–Russian cyber conference that was organized by the East-West Institute of the U.S. and the Information Security Institute of Russia. The definitions were divided into three sections. They were 'the theater' (which included definitions for cyberspace, cyber infrastructure, cyber services, critical cyberspace, critical cyber infrastructure and critical cyber services); 'the modes of aggravation' (cybercrime, cyber terrorism, cyber conflict, cyber war and cyber security); and 'the art' (cyber warfare, cyber attack, cyber counterattack, cyber defensive countermeasure, cyber defense, cyber defensive capability, cyber offensive capability, cyber exploitation and cyber deterrent). The definitions of these terms can be found at www.ewi.info and for that reason are not included in an appendix here.

CONCLUSIONS

Russia is developing a strategy and doctrine to fit its current situation, which is not one of optimism. The military has experienced a series of training catastrophes in almost every area, especially in regard to missile launches and its air mobile assets (helicopters, transport planes, jet aircraft). There has been little integration of assets, particularly communications devices, among services such as the army, air force, and navy and the Ministry of Internal Affairs assets. Instead, the leadership is in the position of applying the strategy of 'playing catch up while limiting others' as best it can through the development of alliance strategies and international information security policies. At the same time, the country hopes to safeguard the advantages it possesses in the absence of international rules and laws, for example, the extended use of surrogates such as the Russian Business Network and other nationalist hacker elements to conduct cyber espionage, which has the potential to yield a treasure house of sensitive information. The Defense Ministry's *Conceptual Views* indicates that the priority principle is 'to collect relevant and reliable information regarding threats', which strongly implies espionage.

Strategy and Doctrine

Russia's cyber strategy and doctrine appears to be multifaceted and consistent. Since the mid-1990s, the nation has pressed an agenda that focuses on information security concepts, as well as terminology. This strategy has involved a host of international security organizations over time and a host of information and cyber proposals. Foremost among the proposals has been the series of international meetings the nation has held at Garmisch, Germany, and in Moscow. Over time, the foreign representation

at these meetings has grown accordingly. Now the U.S. is sending more senior State Department representatives, and an International Information Security Research Consortium has been established. China has now begun to send representatives as well. Overall, the effort has grown appreciably over the past three years. The Russian representatives at this conference on one occasion rank-ordered the topics they deemed the most important for consideration, thereby establishing a strategy of sorts: escalation models, civil infrastructures, definitions, cyber law and codes of conduct were in spots 1–5, respectively. Information warfare deterrence was another important topic. After this initial ranking, spots 6–10 were held by cyber terrorism, cybercrime, technical cooperation, world community protection and industrial espionage, in that order. As mentioned here, however, the principal priority in the *Conceptual Views* document was collecting information on threats. That is, number 10 in the Garmisch priority is number 1 in the *Conceptual Views* document.

The 2010 Russian *Military Doctrine* and the 2009 Russian *National Security Strategy* 2009 offered the clearest explanation of the country's developmental information strategy. The first quotation below is from the doctrine, and the second quotation is from the national security strategy:

> 2010: This included developing forces and resources for information warfare, improving the quality of means of information exchange using up-to-date technologies, creating new models of high-precision weapons, and developing information support for them.

> 2009: The implementation of a series of information measures serve as the basis of this strategy: the harmonization of the national information infrastructure with global information networks and systems; overcoming the technological lag in information science; developing and introducing information security technologies in the state and military administrative systems; increasing the level of protection of corporate and individual information systems; and creating a single information-telecommunications support system for the needs of the national security system.

From a military perspective, the strategy involves a combination of watching and perhaps copying or adjusting some of the concepts that have developed around the world (consideration to create a cyber command, a DARPA, partial acceptance of the network-centric concept, and a concept of information space issues). Also of use are domestic and long-held Soviet and Russian military traditions. The latter include a focus on command and control issues ('victory in a future war will belong to whoever is able, with the greatest effectiveness and coordination, to command and control land, air, sea, and space information issues'), the desire to disorganize an enemy through the use of asymmetric means and the gradual expansion of

the old information-technical and information-psychological concepts into scientific-technical and political-psychological aspects. Other issues are on the horizon. For example, Russian anti-malware expert Eugene Kaspersky noted that the Stuxnet virus marks the beginning of militarily motivated cyber sabotage, which will become a big issue in the coming years. New concept weapons or weapons based on new physical principles are other examples.

Capability in Future Conflict

It appears that during the information warfare or cyber portion of any future conflict, Russia would be able to hold its own. The country has a string of talented algorithm writers who have successfully conducted cyber exploits (Moonlight Maze, etc.) against the U.S. and other nations already. There is a host of online crime figures who are conducting cyber attacks and deceptive information manipulations against Germany and other European nations that have the full attention and professional response of the police in these countries. Russia has significant practical experience to fall back on, whether it be the assault on Estonia a few years ago (which marked a wakeup call for many politicians that there is a political-cyber connection) or the more recent cyber attacks against Georgia during the 2008 war. Finally, several of the top U.S. cyber analysts have placed Russian hackers at the head of the international list of online professionals.

The bottom line is do not count Russia out due to its plethora of IT specialists who are world-renowned for their programming expertise. It takes only one talented algorithm writer to find a way to get into a website or online account or to steal a password and get inside a defense establishment. The IT ability of Russian hackers and other surrogates the nation employs will enable it to stay highly competitive in this area in the coming years. The same cannot be said for other aspects of the Defense Ministry in Russia, which are coping with technical failures (in planes, missiles and other armaments) and reorganization problems.